Application Serial No. 10/560,220   PATENT
Reply to office action of September 2, 2008   Docket: CU-4590

Amendments To The Claims

      The listing of claims presented below will replace all prior versions, and listings,
of claims in the application.

Listing of claims:

1.   **(currently amended)** A rijndael block encryption apparatus having M-bit input
data and N-bit input keys and encrypting the M-bit input data by repeating for a
predetermined number of times a round operation that includes transforms of shift_row,
substitution, mixcolumn and add-round-key, the apparatus comprising:

      a round operation unit including a round operation execution unit for processing
the data in the unit of M/m bits (where m is 2, 3 or 4) at ~~lease~~ least in the transforms of
substitution, mixcolumn and add-round-key, and a round key generation unit for
generating round keys in order to provide the round keys in the transform of the add-
round-key;

      a round operation control unit for controlling the round operation performed by
the round operation unit; and

      a data storage unit for storing ~~M/n-lit~~ **M/m-bit** intermediate data generated by the
round operation unit at an intermediate stage of every round and M-bit data generated
at an end stage of every round,

      **wherein the round keys generated in the add-round-key generation unit is
added to a first M/m input data simultaneously during the processing of a second
M/m input data of the round execution unit before the end stage of every round.**

Page 5 of 18

Application Serial No. 10/560,220   PATENT
Reply to office action of September 2, 2008   Docket: CU-4590

2.   (original) The apparatus as claimed in claim 1, wherein the data storage unit

includes at least one register, and a total summed size of the register is equal to or

larger than M(2m-1)/m bits.

3.   **(currently amended)** A rijndael block decryption apparatus having M-bit input

data and N-bit input keys and decrypting the M-bit input data by repeating for a

predetermined number of times a round operation that includes transforms of inverse

shift_row, inverse substitution, add-round-key and inverse mixcolumn, the apparatus

comprising:

        a round operation unit including a round operation execution unit for processing

the data in the unit of M/m bits (where m is 2, 3 or 4) at ~~lease~~ least in the transforms of

inverse substitution, add-round-key and inverse mixcolumn, and a round key generation

unit for generating round keys in order to provide the round keys in the transform of

add-round-key;

        a round operation control unit for controlling the round operation performed by

the round operation unit; and

        a data storage unit for storing ~~M/n-bit~~ M/m-bit intermediate data generated by

the round operation unit at an intermediate stage of every round and M-bit data

generated at an end stage of every round,

        wherein the round keys generated in the add-round-key generation unit is

added to a first M/m input data simultaneously during the processing of a second

M/m input data of the round execution unit before the end stage of every round.

Page 6 of 18

Application Serial No. 10/560,220   PATENT
Reply to office action of September 2, 2008   Docket: CU-4590

4.   (original) The apparatus as claimed in claim 3, wherein the data storage unit

includes at least one register, and a total summed size of the register is equal to or

larger than M (2m-1)/m bits.

5.   **(currently amended)** A rijndael block cipher apparatus having M-bit input data

and N-bit input keys, and encrypting the M-bit input data by repeating for a

predetermined number of times a round operation for encryption that includes

transforms of shift_row, substitution, mixcolumn and add-round-key or decrypting the M-

bit input data by repeating for a predetermined number of times a round operation for

decryption that includes transforms of inverse shift_row, inverse substitution, add-round-

key and inverse mixcolumn, the apparatus comprising:

      a round operation unit including a round operation execution unit for processing

the data in the unit of M/m bits (where m is 2, 3 or 4) at ~~lease~~ least in the transforms of

substitution, mixcolumn and add-round-key in an encryption mode and for processing

the data in the unit of M/m bits (where m is 2, 3 or 4) at lease in the transforms of

inverse substitution, add-round-key and inverse mixcolumn in a decryption mode, and a

round key generation unit for generating round keys in order to provide the round keys

in the transform of add-round-key;

      a round operation control unit for controlling the round operation performed by

the round operation unit; and

      a data storage unit for storing ~~M/n-bit~~ M/m-bit intermediate data generated by

Page 7 of 18

the round operation unit at an intermediate stage of every round and M-bit data

generated at an end stage of every round,

wherein the round keys generated in the add-round-key generation unit is

added to a first M/m input data simultaneously during the processing of a second

M/m input data of the round execution unit before the end stage of every round.

6.   (original) The apparatus as claimed in claim 5, wherein the round operation

execution unit comprises:

a shift/inverse-shift_row operation means for performing the shift_row operation

and the inverse shift_row operation of the data;

a substitution/inverse-substitution operation means for performing the

substitution operation and the inverse substitution operation of the data;

a mixcolumn/inverse-mixcolumn operation means for performing the mixcolumn

operation and the inverse mixcolumn operation of the data; and

an add-round-key operation means for performing the add-round-key operation

of the data.

7.   (original) The apparatus as claimed in claim 6, wherein the round operation

execution unit further comprises a plurality of demultiplexing means for controlling a flow

of the data among the substitution/inverse-substitution operation means, the

mixcolumn/inverse-mixcolumn operation means and the add-round-key operation

means so as to perform the round operation for the encryption or the round operation

Page 8 of 18

Application Serial No. 10/560,220   PATENT
Reply to office action of September 2, 2008   Docket: CU-4590

for the decryption according to an input of a mode signal that indicates the encryption or decryption mode.

8.   (original) The apparatus as claimed in any one of claims 5 to 7, wherein the data storage unit includes at least one register, and a total summed size of the register is equal to or larger than $M(2m-1)/m$ bits.

9.   **(currently amended)** A rijndael block encryption method for receiving M-bit input data and N-bit input keys and performing a round operation of the input data for a predetermined number of times, the method comprising:

a round operation step of performing a round operation with respect to all m data of M/n bits, the round operation including sub-steps of a shift_row transform for performing a shift_row of the M-bit data from a previous round and outputting only M/m-bit (where m is 2, 3 and 4) data corresponding to a selection signal to a next step, a substitution transform for performing a substitution of the M/m-bit data, a mixcolumn transform for performing a mixcolumn of the M/m-bit data, and an add-round-key transform for performing an addition of round keys having the same size to the M/m-bit data, respectively; and

a round key generation step of generating the round keys in order to provide the round keys at the sub-step of the add-round-key transform,

wherein the round keys generated in the add-round-key generation unit is added to a first M/m input data simultaneously during the processing of a second

Page 9 of 18

Application Serial No. 10/560,220   PATENT
Reply to office action of September 2, 2008   Docket: CU-4590

M/m input data of the round execution unit before the end stage of every round.

10.   (original) The method as claimed in claim 9, wherein the data having the size of

M/m bits can be processed through the steps of the shift_row transform, the substitution

transform, the mixcolumn transform and the add-round-key transform, respectively, and

a plurality of the M/m-bit data can be processed through the plural steps selected

among the four steps at the same time according to a predetermined timing.

11.   **(currently amended)** A rijndael block decryption method for receiving M-bit input

data and N-bit input keys and performing a round operation of the input data for a

predetermined number of times, the method comprising:

a round operation step of performing a round operation with respect to all m data

of M/n bits, the round operation including sub-steps of an inverse shift_row transform for

performing an inverse shift_row of the M-bit data from a previous round and outputting

only M/m-bit (where m is 2, 3 and 4) data corresponding to a selection signal to a next

step, an inverse substitution transform for performing an inverse substitution of the M/m-

bit inverse-shift_row-transformed data, an add-round-key transform for performing an

addition of round keys having the same size to the M/m-bit inverse-substitution-

transformed data, respectively, and an inverse mixcolumn transform for performing an

inverse mixcolumn of the M/m-bit add-round-key-transformed data; and

a round key generation step of generating the round keys in order to provide the

round keys at the sub-step of the add-round-key transform,

Application Serial No. 10/560,220   PATENT
Reply to office action of September 2, 2008   Docket: CU-4590

wherein the round keys generated in the add-round-key generation unit is

added to a first M/m input data simultaneously during the processing of a second

M/m input data of the round execution unit before the end stage of every round.

12.   (original) The method as claimed in claim 11, wherein the data having the size of

M/m bits can be processed through the steps of the inverse shift_row transform, the

inverse substitution transform, the add-round-key transform and the inverse mixcolumn

transform, respectively, and a plurality of the M/m-bit data can be processed through the

plural steps selected among the four steps at the same time according to a

predetermined timing.